#4
BT
2151
12-13-02

THOMPSON & KNIGHT
LLP
ATTORNEYS AND COUNSELORS

1200 SAN JACINTO CENTER
98 SAN JACINTO BOULEVARD
AUSTIN, TEXAS 78701-4081
(512) 469-6100
FAX (512) 469-6180
www.tklaw.com

AUSTIN
DALLAS
FORT WORTH
HOUSTON
MONTERREY, MEXICO

RECEIVED
DEC 0 3 2002
Technology Center 2100

November 27, 2002

Commissioner for Patents
Washington, DC 20231

RE: SN 10/068,295 "APPLICATION-SPECIFIC INFORMATION-PROCESSING METHOD, SYSTEM AND APPARATUS"- Oscar R. Mitchell et al
(Our File No. 501143.000019)

Sir:

Enclosed for filing in connection with the above-referenced patent application are:

1.   Information Disclosure Statement (PTO/SB/08A); 3 pages

2.   Copies of documents A1 – A13; C1 – C20 cited in the Information Disclosure Statement; and

3.   Return receipt postcard.

In accordance with 37 C.F.R §§ 1.97(g),(h), the enclosed Information Disclosure Statement is not to be construed as a representation that a search has been made, and is not to be construed to be an admission that the information cited is, or is considered to be, material to patentability as defined in 37 C.F.R. § 1.56(b).

The Information Disclosure Statement is being filed prior to the receipt of a first Office Action reflecting an examination on the merits, and hence is believed to be timely filed in accordance with 37 C.F.R § 1.97(b).

No fees are believed to be due in connection with the filing of these documents. However, should any fees under 37 C.F.R. §§ 1.16 to 1.21 be deemed necessary for any reason relating to

the enclosed materials, the Commissioner for Patents is hereby authorized to deduct said fees from Thompson & Knight, L.L.P.'s Deposit Account No. 20-0821/501143.000019/AAW.

Applicants respectfully request that the listed documents be made of record in the present case. Please date stamp and return the enclosed postcard evidencing receipt of these materials.

Respectfully submitted,

Aaron A. Weiss
Reg. No. 46,163

AAW:ce
Encl.

Substitute for form 1449A/PTO			**Complete if Known**		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (use as many sheets as necessary)			Application Number	10/068,295	RECEIVED
			Filing Date	February 5, 2002	
			First Named Inventor	Mitchell, Oscar	DEC 03 2002
			Art Unit	2151	
			Examiner Name		Technology Center 2100
Sheet	1	of 3	Attorney Docket Number	501143.000019	

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number- Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1	US- 6,341,299	01-22-2002	Romain	
	A2	US- 6,157,955	12-05-2000	Narad et al	
	A3	US- 6,151,393	11-21-2000	Jeong	
	A4	US- 6,141,705	10-31-2000	Anand et al	
	A5	US- 6,134,244	10-17-2000	Van Renesse et al	
	A6	US- 6,088,453	07-11-2000	Shimbo	
	A7	US- 5,987,574	11-16-1999	Paluch	
	A8	US- 5,983,299	11-09-1999	Qureshi	
	A9	US- 5,764,554	06-09-1998	Monier	
	A10	US- 5,724.279	03--03-1998	Benaloh et al	
	A11	US- 5,699,537	12-16-1997	Sharangpani et al	
	A12	US- 5,542,061	07-30-1996	Omata	
	A13	US- 4,799,149	01-17-1989	Wolf	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] -Number[4]- Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

Substitute for form 1449B/PTO	**Complete if Known**	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Application Number	10/068,295
	Filing Date	February 5, 2002
	First Named Inventor	Mitchell, Oscar
	Group Art Unit	2151
(use as many sheets as necessary)	Examiner Name	
Sheet	2	of	3	Attorney Docket Number	501143.000019

RECEIVED DEC 3 2002 Technology Center 2100

OIPE DEC 0 2 2002

OTHER PRIOR ART -- NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C1	MENEZES, A.J., et al "Efficient Implementation" from theHandbook of Applied Cryptography, (Boca Raton, CRS Press, 1997), pp. 591-607.	
	C2	DIMITROV, V. and COOKLEV, T., "Two Algorithms for Modular Exponentiation Using Nonstandard Arithmetics" IEICE Trans. Fundamentals, Vol. E78-A, No. 1, January 1995.	
	C3	KOC, C.K. and HUNG, C.Y., "Carry-Save Adders for Computing the Product AB Modulo N" Electronics Letters, Vol. 26, No. 13, (June 21, 1990), pp. 899-900	
	C4	FREKING, W. L. and PARHI, K.K., " Montgomery Modular Multiplication and Exponentiation in the Residue Number System" Proc. 33rd Asilomar Conf. Signals Systems and Computer, October 1999, pp. 1312-1316.	
	C5	TENCA, A.F. and KOC, C.K., "A Scalable Architecture for Montgomery Multiplication" in: KOC, C.K. and PAAR, C., Cryptographic Hardware and Embedded Systems, CHES 99, Lecture Notes in Computer Science, No. 1717. 1998, New York, NY: Springer-Verlog, 1999.	
	C6	KOC, C.K. and ACAR, T., " Montgomery Multiplication in GF (2k)" 3rd Annual Workshop on Selected Areas in Cryptography, (August 15-16, 1996), pp. 95-106.	
	C7	BAJARD, J.C., et al "An RNS Montgomery Modular Multiplication Algorithm" IEEE Transactions on Computer, Vol. 47, No. 7, (July 1998), pp. 766-776.	
	C8	ELDRIDGE, S.E., "A Faster Modular Multiplication Algorithm" International Journal of Computer Math, Vol. 40, (1991), pp. 63-68.	
	C9	BOSSALAERS, A.., et al "Comparison of Three Modular Reduction Functions" In Douglas R. Stinson, editor, Advances in Cryptology - - CRYPTO '93, Vol. 773 of Lecture Notes in Computer Science, (August 22-26, 1993), pp. 166-174.	
	C10	MONTGOMERY, P.L., "Modular Multiplication Without Trial Division" Mathematics of Computation, Vol. 44, No. 170 (April 1985), pp. 519-521.	
	C11	KOC, C.K., et al "Analyzing and Comparing Montgomery Multiplication Algorithms" IEEE Micro, Vol. 16, Issue 3, (June 1996), pp. 26-33.	

Examiner Signature		Date Considered	

RECEIVED
DEC 03 2002
Technology Center 2100

Substitute for form 1449B/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Application Number	10/068,295
	Filing Date	February 5, 2002
	First Named Inventor	Mitchell, Oscar
	Group Art Unit	2151
(use as many sheets as necessary)	Examiner Name	
Sheet 3 of 3	Attorney Docket Number	501143.000019

OTHER PRIOR ART -- NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C 12	KORNERUP, P., " High-Radix Modular Multiplication for Cryptosystems" Department of Mathematics and Computer Science, (1993), pp. 277-283.	
	C 13	SUNAR, B. and KOC, C.K., "An Efficient Optimal Normal Basis Type II Multiplier" Brief Contributions, IEEE Transactions on Computers, Vol. 50, No. 1, (January 2001), pp. 83-87.	
	C 14	KOC, C.K., "Comments on' Residue Arithmetic VLSI Array Architecture for Manipulator Pseudo-Inverse Jacobian Computation' " Communications, IEEE Transactions on Robotics and Automation, Vol. 7, No. 5, (October 1991), pp. 715-716.	
	C 15	SAVAS, E. and KOC, C.K., "The Montgomery Modular Inverse-Revisited" IEEE Transactions on Computers, Vol. 49, No. 7, (July 2000), pp. 763-766.	
	C 16	WALTER, C.D., " Montgomery's Multiplication Technique: How to Make it Smaller and Faster" in Cryptographic Hardware and Embedded Systems - CHAS 1999, C. Paar (Eds.). K. Ko, Ed. 1999, Springer, Berlin Germany, pp.61-72.	
	C 17	OH, H. and MOON, J., "Modular Multiplication Method" IEE Proc.-Comput. Digit.Tech., Vol. 145, No. 4, (July 1998), pp. 317-318.	
	C 18	BLUM, T., " Modular Exponentiation on Reconfigurable Hardware" Master's thesis, ECE Department, Worcester Polytechnic Institute, Submitted to Faculty 1999-04-08, Published May 1999. Retrieved from the Internet <URL: http://www.wpi.edu/pubs/ETD/Available/etd-090399-090413/unrestricted/blum.pdf>.	
	C 19	MARWEDEL, P., et al. "Built in Chaining: Introducing Complex Components into Architectural Synthesis." April 1996. Proceedings of the ASP-DAC, 1997. [online]. Retrieved from the Internet <URL: http://eldorado.uni-dortmund.de:8080/FB4/ls12/forshung/1997/aspdac/aspacPDF>.	
	C 20	TIOUNTCHIK, A., and TRICHINA, E., "RSA Acceleration with Field Programmable Gate Arrays" Lecture Notes in Computer Science, Vol. 1587, pp.164-176. Retrieved from the Internet: <URL:http://citeseer.nj.nec.com/274658.html>.	

Examiner Signature		Date Considered	